Kentucky Department of Education

Our Children,
Our Commonwealth

KSIS CLOUD DISTRICT TECHNICAL REFERENCE

5/10/17

Table of Contents

Introduction

This document describes the integration of the Kentucky Student Information System, using the Infinite Campus Private Cloud, with other KETS components. It is directed at technology staff who must support district users of KSIS and the integration of other systems with KSIS. This document is a supplement to Infinite Campus-provided documentation.

Update History

6 March 2017 – Initial Release

10 May 2017 – Describe New LDAP Authentication configuration

Network

By design, the vast majority of Campus-related network traffic to/from district-connected devices will pass through the KETS wide area network (KEN) and its public Internet connection. A small amount of traffic will travel through a VPN (Virtual Private Network) connection between KEN and Infinite Campus' datacenter.

Workstation/Browser Configuration

No KETS-specific workstation/browser configuration should be necessary. Search Campus Community for "Supported Platforms" and "Recommended Browser Settings".

Internet Content Management (Lightspeed)

No Campus-specific configuration should be required on the Lightspeed-based KETS Internet Content Management system.

Integration with KETS Active Directory using SAML

At this time, KETS does not support or recommend use of Campus' SAML functionality for integration with KETS Active Directory.

Old Integration with KETS Active Directory using LDAP

General information about this integration feature is available in the Campus Community; search for “Old LDAP Authentication”. Note that the following information describes what is now known as the “Old LDAP Authentication” feature which will only be available until late summer of 2017; the next section of this document addresses the newer LDAP Authentication configuration options that became available in Campus release .1701.

Benefits of AD Integration

- Users do not need to remember a second IC password or manually keep two passwords in sync.
- IC passwords will effectively be subject to the same password policies as AD passwords with no additional management effort.
- Passwords are stored securely and there is no need for users to periodically change their IC password.
- Administrators can disable a user’s access to AD/Email and IC with one step for users set up to use LDAP authentication.

Frequently Asked Questions

1. Does AD Integration affect Parent/Student Portal Access?

Yes. If a district chooses to migrate students to AD integration, those students will need to use their AD credentials to log into the Student Portal. District Staff who use the Parent Portal will need to use their AD credentials. Parents who do not have AD accounts will NOT use AD credentials and will continue to log in with their existing credentials.

2. Does AD Integration affect an administrator’s ability to “Login as User” within Infinite Campus?

No, “Login as User” continues to work as before even if the user has been migrated to AD integration.

3. Can a user be switched back to a Campus-specific username once they have been configured for AD integration?

Yes, but only using the Account Editor screen, not using the Account Settings screen.

4. Will AD Integration and Campus Password Reset functionality conflict with each other?

No, but users will only be able to use the Campus Password Reset functionality if their Campus account is NOT integrated with Active Directory. A district can choose to have some users integrated with Active Directory and others using Campus passwords and Campus Password Reset functionality.

Planning Considerations

1. When implementing AD integration, it is ESSENTIAL to create or retain an administrative-level Infinite Campus user that is NOT linked with Active Directory. In case of an AD connectivity issue, this account may be the only one that can be used to adjust the Infinite Campus configuration.
2. After switching to AD integration, consider removing the “Account Settings” Tool Right from most groups so that users do not try to change their passwords (which will not be effective) or change their LDAP connections.
3. The Campus LDAP documentation mentions the possible need to make firewall adjustments; no adjustments should be required in the KETS environment.
4. Be cautious about deleting and recreating an AD account that is linked to an Infinite Campus account; depending on the order of events you may be required to recreate the Infinite Campus account after recreating the AD account.
5. Even though users can log into Windows using multiple forms of their username (such as logon/SAMAccountName, User Principal Name, and primary SMTP address), they will only be able to log into Infinite Campus using the attribute specified in the Campus LDAP configuration screen.
6. If there is ever a need to remove AD integration, you must ensure that each user has an appropriate password set on their Campus user before disconnecting the user from Active Directory.
7. You may implement AD integration for students (for access to the Parent/Student Portal) as well as for district staff users.
8. In a Disaster Recovery scenario in which Campus is temporarily hosting the district’s installation, AD integration will be disabled. Infinite Campus Hosting will set a unique password on each Campus user and provide a list of all usernames and passwords to the district contact for distribution to users.
9. LDAP authentication to KETS AD servers requires proper Windows licensing. All students and non-employees are covered by KETS-provided external connector licenses; districts must ensure that all employees using LDAP authentication are covered by district-purchased Windows CALs.
10. The “Expires Date” field on the User Account screen will still be effective for a user that has migrated to AD (though it only affect the ability to log into Campus); Infinite

Campus considers this a bug and in some future version this field will no longer have any effect.

11. Consider whether you want to start requiring stronger AD passwords as part of the migration. Section 3.1.5 of the KETS Active Directory Operations Guide (available at www.education.ky.gov) describes options for requiring stronger AD passwords.
12. Every character that appears on a standard Windows keyboard can be used in an AD password for an account that is integrated with Infinite Campus. Other characters (such as symbols generated with the Alt key) have not been tested.
13. Campus will lock out a user account after 5 failed login attempts even if the user account is integrated with AD. When this happens an administrator will have to unlock the Campus user account in addition to unlocking the AD account. Consider whether you wish to reduce the AD threshold for failed login attempts to a smaller value than 5 in order to help prevent this. Infinite Campus considers this a bug and in some future version the Campus system will not lock out Campus user accounts for AD-integrated users.
14. The password for the Bind User (an AD account used by Campus for Active Directory lookups in certain situations) is stored in plain text within the Campus database. Infinite Campus will modify the product to store this password securely in a future version.
15. Campus has placed code in their login page that blocks the browser from remembering the username, such that every time a user wants to log into Campus, they have to type all of the username and password.
16. If an AD-integrated user's username is changed in Active Directory, the user will need to log into Infinite Campus one more time using the prior username in order for Campus to properly update the link; after that one time the new AD username must be used for Campus login.

Configuration Recommendations

These recommendations apply specifically to the one-time system-wide configuration described in Campus documentation.

1) Host priority	Locally Hosted Districts: Specify the district DC (Domain Controller) as Server 1 Host, GC (Global Catalog) as Server 2 Host, using fully-qualified domain names (for example, ed999addc1.kets.ketsds.net). Cloud Districts: Contact Campus Support through normal channels and request the surrogate (Network Address Translation, aka NAT) IP addresses that will allow your cloud-located installation to connect to your district's AD servers.
2) Port	Specify 636 for both servers to support SSL.

3) SSL	Check the box to specify SSL. The necessary certificates for LDAP communication over SSL are already in place on all KETS domain controllers.
4) Bind User	This AD account will be used by the Infinite Campus software to query Active Directory. This account does not need any AD permissions beyond the default granted to all AD accounts. This is a service account and should be configured to not expire password and to not require password change on first login. Object name: IC_Integration_Bind_User Object OU: _District Admins/Service Accounts
5) Bind Password	This account should be given a strong (long, complex) password since the password cannot be changed frequently.
6) Search Base	This identifies the level on the AD tree from which Infinite Campus will begin searches when attempting to match Campus users to AD users. The recommended value is DC=*districtname*,DC=ketsds,DC=net Where *districtname* is the district AD domain name.
7) Username Attribute	The recommended value is userPrincipalName so that users can log into Campus using their email address, just as they log into Office 365.

Migration Options

You have three options for the actual process of migrating users to Active Directory Authentication.

1. An administrator can edit each existing Campus user account. Further details are available in the Campus LDAP Authentication documentation.
2. Each user can edit their own Campus user account. Further details are available in the Campus LDAP Authentication documentation.
3. Scripted migration through Campus Support and Data Conversion groups. Further details are found below.

NOTE: The user’s Microsoft Office 365 email address must be used as the Campus username if choosing the Scripted Migration Option.

Scripted Migration Options

KDE will pay for each district to use the scripted migration process to connect your Campus usernames to Active Directory accounts. If you wish to use the scripted process, you will need to follow these steps:

1. Retrieve the Staff and optionally the Student file from https://live.kyschools.us/ADIC. Any district user can access these files by logging in with their Office 365 username and password (note that depending on your browser you may have to authenticate several times). The three-digit district number is part of the filename. The data in these files is available to any district user by connecting to Active Directory but is assembled in these files for convenience. These files are updated nightly.
2. Review the files (which are in CSV [Comma Separated Values] format) using Excel or a text editor and remove the rows for any Campus users that should NOT be integrated with Active Directory. Rows whose email addresses cannot be found in Campus will be skipped by the migration process and listed in a provided report.
3. Verify that you have correct Office 365 email addresses attached to each Campus user to be integrated with Active Directory.
4. Decide if you are going to have the Data Conversion group migrate your Campus Sandbox installation first. A Sandbox migration can help you find any issues in your existing user accounts before performing a Production migration, but is not required.
5. Open a ticket with Campus Support, titling it "AD Authentication Migration for *districtname*", specifying preference for Sandbox migration or not, whether you're migrating Staff only or Staff and Students, and uploading the edited CSV files.
6. If you have requested a Sandbox migration, Campus Hosting will refresh your Sandbox and Campus Data Conversion will execute the migration in the Sandbox and provide a report of the results through your Support Ticket. Review the results and make any appropriate changes in Infinite Campus and/or Active Directory.
7. Update your Campus Support ticket with at least three possible dates for your Production migration. Campus Data Conversion will respond and any further timing details will be settled through the Support ticket.
8. Communicate with your users regarding the upcoming change in login process and any changes to Active Directory password policies.
9. Complete the one-time system-wide configuration described in section "Configuring Campus for LDAP Authentication" of the Campus document *LDAP Authentication*, referencing the configuration recommendations listed above.
10. Shortly before your Production migration, download fresh versions of the Staff and (optionally) Student files, remove rows for any Campus users that should NOT be integrated with Active Directory, and upload them to your existing Support ticket.

11. Campus Data Conversion will execute the migration in Production and provide a report of the results through your Support ticket.
12. Provide any follow-up communication to your users.

Support

For Campus product functionality support, please contact Infinite Campus Support through the usual channels.

For questions about this document, issues with the Staff and Student files provided by KDE, or other support needs related to integration in the KETS environment, please contact the KETS Service Desk at KETSHelp@education.ky.gov.

New Integration with KETS Active Directory using LDAP

General information about this integration feature is available in the Campus Community; search for “LDAP Authentication” and ignore any documents labeled “Old LDAP Authentication”. Note that the following information describes the newer LDAP Authentication configuration options that became available in Campus release .1701; the prior section of this document addresses what is now known as the “Old LDAP Authentication” feature.

Benefits of AD Integration

- Users do not need to remember a second IC password or manually keep two passwords in sync.

- IC passwords will effectively be subject to the same password policies as AD passwords with no additional management effort.

- Passwords are stored securely and there is no need for users to periodically change their IC password.

- Administrators can disable a user’s access to AD/Email and IC with one step for users set up to use LDAP authentication.

Frequently Asked Questions

1. Does AD Integration affect Parent/Student Portal Access?

Yes. If a district chooses to migrate students to AD integration, those students will need to use their AD credentials to log into the Student Portal. District Staff who use the

Parent Portal will need to use their AD credentials. Parents who do not have AD accounts will NOT use AD credentials and will continue to log in with their existing credentials.

2. Does AD Integration affect an administrator's ability to "Login as User" within Infinite Campus?

No, "Login as User" continues to work as before even if the user has been migrated to AD integration.

3. Can a user be switched back to a Campus-specific username once they have been configured for AD integration?

Yes.

4. Will AD Integration and Campus Password Reset functionality conflict with each other?

No, but users will only be able to use the Campus Password Reset functionality if their Campus account is NOT integrated with Active Directory. A district can choose to have some users integrated with Active Directory and others using Campus passwords and Campus Password Reset functionality.

Planning Considerations

1. When implementing AD integration, it is **ESSENTIAL** to create or retain an administrative-level Infinite Campus user that is NOT linked with Active Directory. In case of an AD connectivity issue, this account may be the only one that can be used to adjust the Infinite Campus configuration.
2. The Campus LDAP documentation mentions the possible need to make firewall adjustments; no adjustments should be required in the KETS environment.
3. Be cautious about deleting and recreating an AD account that is linked to an Infinite Campus account; depending on the order of events you may be required to recreate the Infinite Campus account after recreating the AD account.
4. Even though users can log into Windows using multiple forms of their username (such as logon/SAMAccountName, User Principal Name, and primary SMTP address), they will only be able to log into Infinite Campus using the attribute specified in the Campus LDAP configuration screen.
5. If there is ever a need to remove AD integration, you must ensure that each user has an appropriate password set on their Campus user before disconnecting the user from Active Directory.
6. You may implement AD integration for students (for access to the Parent/Student Portal and Mobile Portal app) as well as for district staff users.

7. LDAP authentication to KETS AD servers requires proper Windows licensing. All students and non-employees are covered by KETS-provided external connector licenses; districts must ensure that all employees using LDAP authentication are covered by district-purchased Windows CALs.
8. The “Expires Date” field on the User Account screen will still be effective for a user that has migrated to AD (though it only affect the ability to log into Campus); Infinite Campus considers this a bug and in some future version this field will no longer have any effect.
9. Consider whether you want to start requiring stronger AD passwords as part of the migration. Section 3.1.5 of the KETS Active Directory Operations Guide (available at www.education.ky.gov) describes options for requiring stronger AD passwords.
10. Every character that appears on a standard Windows keyboard can be used in an AD password for an account that is integrated with Infinite Campus. Other characters (such as symbols generated with the Alt key) have not been tested.
11. Campus will lock out a user account after 5 failed login attempts even if the user account is integrated with AD. When this happens an administrator will have to unlock the Campus user account in addition to unlocking the AD account. Consider whether you wish to reduce the AD threshold for failed login attempts to a smaller value than 5 in order to help prevent this. Infinite Campus considers this a bug and in some future version the Campus system will not lock out Campus user accounts for AD-integrated users.
12. The password for the Bind User (an AD account used by Campus for Active Directory lookups in certain situations) is stored in plain text within the Campus database. Infinite Campus will modify the product to store this password securely in a future version.
13. Campus has placed code in their login page that blocks the browser from remembering the username, such that every time a user wants to log into Campus, they have to type all of the username and password.
14. If an AD-integrated user’s username is changed in Active Directory, the user will need to log into Infinite Campus one more time using the prior username in order for Campus to properly update the link; after that one time the new AD username must be used for Campus login.
15. If an AD-integrated user’s Active Directory object is moved from one OU to another within Active Directory, the user may not be able to log into Campus for up to 15 minutes due to AD replication configuration.

Configuration Recommendations

These recommendations apply specifically to the one-time system-wide configuration described in Campus documentation. For items that are not addressed below, consult the Campus documentation; there are no KETS-specific recommendations for these items.

1) LDAP Server Pool Hosts	Locally Hosted Districts: Specify the district domain controllers (DC1, DC3, GC1), using fully-qualified domain names (for example, ed999addc1.kets.ketsds.net). The order does not matter as Campus software will distribute requests to all domain controllers equally (unless one of them becomes unresponsive). Cloud Districts: Contact Campus Support through normal channels and request the surrogate (Network Address Translation, aka NAT) IP addresses that will allow your cloud-located installation to connect to your district's AD servers. The order does not matter as Campus software will distribute requests to all domain controllers equally (unless one of them becomes unresponsive).
2) Port	Specify 636 for each server to support SSL.
3) Use SSL	Check the box to specify SSL. The necessary certificates for LDAP communication over SSL are already in place on all KETS domain controllers.
4) Bind User DN	This AD account will be used by the Infinite Campus software to query Active Directory. This account does not need any AD permissions beyond the default granted to all AD accounts. This is a service account and should be configured to not expire password and to not require password change on first login. Note: The value for this field MUST be a fully qualified Distinguished Name, for example: CN= IC_Integration_Bind_User,OU=Service Accounts,OU=_District Admins,DC=*districtname*, DC=ketsds,DC=net Neither AD short name nor User Principal Name (email address) will work. Recommended Object name: IC_Integration_Bind_User (entered as full Distinguished Name as noted above) Recommended Object OU: _District Admins/Service

	Accounts **WARNING:** Because the full Distinguished Name is used, if this AD account is moved to a different OU, the Campus configuration MUST be updated with the new DN.
5) Bind User Password	This account should be given a strong (long, complex) password since the password cannot be changed frequently.
6) User Search Base	This identifies the level on the AD tree from which Infinite Campus will begin searches when attempting to match Campus users to AD users. The recommended value is DC=*districtname*,DC=ketsds,DC=net Where *districtname* is the district AD domain name.
7) User Search Filter	The recommended value is (UserPrincipalName={0}) so that users can log into Campus using their email address, just as they log into Office 365.

Migration Options

You have two options for the actual process of migrating users to Active Directory Authentication.

1. An administrator can edit existing Campus user accounts, either individually or en masse. Further details are available in the Campus LDAP Authentication documentation.
2. Scripted migration through Campus Support and Data Conversion groups. Further details are found below.

> ***NOTE:*** The user's Microsoft Office 365 email address must be used as the Campus username if choosing the Scripted Migration Option.

Scripted Migration Options

KDE will pay for each district to use the scripted migration process to connect your Campus usernames to Active Directory accounts. If you wish to use the scripted process, you will need to follow these steps:

1. Retrieve the Staff and optionally the Student file from https://live.kyschools.us/ADIC. Any district user can access these files by logging in with their Office 365 username

and password (note that depending on your browser you may have to authenticate several times). The three-digit district number is part of the filename. The data in these files is available to any district user by connecting to Active Directory but is assembled in these files for convenience. These files are updated nightly.

2. Review the files (which are in CSV [Comma Separated Values] format) using Excel or a text editor and remove the rows for any Campus users that should NOT be integrated with Active Directory. Rows whose email addresses cannot be found in Campus will be skipped by the migration process and listed in a provided report.
3. Verify that you have correct Office 365 email addresses attached to each Campus user to be integrated with Active Directory.
4. Decide if you are going to have the Data Conversion group migrate your Campus Sandbox installation first. A Sandbox migration can help you find any issues in your existing user accounts before performing a Production migration, but is not required.
5. Open a ticket with Campus Support, titling it "AD Authentication Migration for *districtname*", specifying preference for Sandbox migration or not, whether you're migrating Staff only or Staff and Students, and uploading the edited CSV files. Include the LDAP configuration name so Campus Support can create the LDAP configuration relationships between the user accounts and the proper LDAP configuration.
6. If you have requested a Sandbox migration, Campus Hosting will refresh your Sandbox and Campus Data Conversion will execute the migration in the Sandbox and provide a report of the results through your Support Ticket. Review the results and make any appropriate changes in Infinite Campus and/or Active Directory.
7. Update your Campus Support ticket with at least three possible dates for your Production migration. Campus Data Conversion will respond and any further timing details will be settled through the Support ticket.
8. Communicate with your users regarding the upcoming change in login process and any changes to Active Directory password policies.
9. Complete the one-time system-wide configuration described in section "Configuring Campus for LDAP Authentication" of the Campus document *LDAP Authentication*, referencing the configuration recommendations listed above.
10. Shortly before your Production migration, download fresh versions of the Staff and (optionally) Student files, remove rows for any Campus users that should NOT be integrated with Active Directory, and upload them to your existing Support ticket.
11. Campus Data Conversion will execute the migration in Production and provide a report of the results through your Support ticket.
12. Test the configuration by going into the LDAP Authentication configuration tab and select a valid username for testing. This will ensure that the LDAP protocol is successfully executing between Infinite Campus and KETS.
13. Provide any follow-up communication to your users.

Support

For Campus product functionality support, please contact Infinite Campus Support through the usual channels.

For questions about this document, issues with the Staff and Student files provided by KDE, or other support needs related to integration in the KETS environment, please contact the KETS Service Desk at KETSHelp@education.ky.gov.

Campus Data Extract Utility

Detailed documentation of the Campus Data Extract Utility is available in Campus Community; search for “Data Extract Utility (Custom Development)”.

SMB Delivery Mode

The SMB delivery mode causes the Campus servers to place the extract file on an in-district Windows file server using standard Windows file sharing (no additional software required). SMB will eventually be retired as an option for Kentucky cloud districts.

Use of SMB requires a surrogate (Network Address Translation) IP address which allows the Campus servers to connect to the district’s Windows file server through a VPN connection between Campus and Kentucky (KEN). This surrogate IP address is entered in the Data Extract Utility interface only; the locally configured IP address of the Windows file server is NOT changed.

In order to request a surrogate IP address, contact Campus support through the usual channels and provide the locally configured IP address and name of the Windows file server. Up to three surrogate IP addresses can be provided per district (including those used for Eligibility Import, discussed later).

Secure FTP Delivery Modes

The two secure FTP delivery modes (SFTP and FTPS) cause the Campus servers to place the extract file on a secure FTP site of the district’s choosing. Both types of secure FTP require installing and configuring software on a server. Neither Campus nor KETS can provide assistance with procuring, installing, configuring, or operating secure FTP software. However, for secure FTP sites on a district-located server, the KETS Service Desk can assist with configuration changes to the KETS firewall and the allocation of a public IP address.

The Campus Cloud servers’ public IP addresses (from which secure FTP connections will originate) will be from one or more of these ranges:

65.124.140.0/24
207.225.137.0/24

198.73.96.0/21

216.226.196.0/22

FRAM Eligibility Import Wizard Scheduled Imports

Detailed documentation of the Campus FRAM Eligibility Import Wizard Scheduled Imports feature is available in Campus Community.

SMB Protocol

The SMB protocol causes the Campus servers to import the data file from an in-district Windows file server using standard Windows file sharing (no additional software required). SMB will eventually be retired as an option for Kentucky cloud districts.

Use of SMB requires a surrogate (Network Address Translation) IP address which allows the Campus servers to connect to the district's Windows file server through a VPN connection between Campus and Kentucky (KEN). This surrogate IP address is entered in the Scheduled Imports interface only; the locally configured IP address of the Windows file server is NOT changed.

In order to request a surrogate IP address, contact Campus support through the usual channels and provide the locally configured IP address and name of the Windows file server. Up to three surrogate IP addresses can be provided per district (including those used for Data Extracts, discussed earlier).

Secure FTP Protocol

The secure FTP (FTPS) protocol causes the Campus servers to import the data file from a secure FTP site of the district's choosing. Secure FTP (FTPS) requires installing and configuring software on a server. Neither Campus nor KETS can provide assistance with procuring, installing, configuring, or operating secure FTP software. However, for secure FTP sites on a district-located server, the KETS Service Desk can assist with configuration changes to the KETS firewall and the allocation of a public IP address.

Note that the SFTP protocol is NOT supported by the Scheduled Imports feature.

The Campus Cloud servers' public IP addresses (from which secure FTP connections will originate) will be from one or more of these ranges:

65.124.140.0/24

207.225.137.0/24

198.73.96.0/21

216.226.196.0/22

Email Messenger SMTP Relay Configuration

Detailed documentation of the Campus Email configuration is available in Campus Community; search for “Email Settings”.

Campus provides an SMTP Relay that can be used as the “SMTP Host”, though districts may choose to use another SMTP Relay instead.

If changing the SMTP Relay, contact the KETS Service Desk to have the district’s SPF (Sender Policy Framework) DNS record updated appropriately.